ICS

|  |
| --- |
| CCS       |

DB51

川渝地区地方标准

DB 51/T XXXX—2023

DB 50/T XXXX—2023

|  |
| --- |
|       |

川渝政务数据风险评估指南

（征求意见稿）

|  |
| --- |
|  |
|       |

XXXX - XX - XX发布

XXXX - XX - XX实施

四川省市场监督管理局

重庆市市场监督管理局

发布

目 录

[目 录 2](#_Toc136604962)

[前 言 3](#_Toc136604963)

[引 言 4](#_Toc136604964)

[1 范围 5](#_Toc136604965)

[2 规范性引用文件 5](#_Toc136604966)

[3 术语和定义 5](#_Toc136604967)

[4 政务数据风险评估工作概述 6](#_Toc136604968)

[5 政务数据风险评估工作实施 11](#_Toc136604969)

[附录A （资料性） 自评估和检查评估实施步骤 17](#_Toc136604970)

[附录B （资料性） 典型数据安全风险类别 18](#_Toc136604971)

[附 录 C （资料性） 政务数据风险评估报告模板 20](#_Toc136604972)

[附 录 D （资料性） 政务数据安全工作评估得分表模板 21](#_Toc136604973)

[参考文献 22](#_Toc136604974)

前 言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分: 标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由四川省大数据中心、重庆市大数据应用发展管理局联合提出、归口并组织实施。

本文件起草单位: 四川省发展和改革委员会、四川省互联网信息办公室、重庆市互联网信息办公室、四川省大数据中心、重庆市大数据应用发展管理局、四川省标准化研究院、国家计算机网络与信息安全管理中心四川分中心、中电科网络安全科技股份有限公司。

本文件主要起草人:魏杰、赵衍、李蒙、李坪芮、余靖浊、周立、黄智勇、高屹嵩、李贝贝、牛灏等。

本文件为首次制定发布。

引 言

政务数据风险评估是政务数据安全保障体系的重要环节，主要针对政务数据处理者的政务数据和政务数据处理活动进行风险评估，区别于相关部门针对数据处理活动违法违规所进行的执法检查，风险评估旨在掌握政务数据安全总体状况，发现政务数据安全隐患，提出政务数据安全管理和技术防护措施建议。结合川渝地区实际，规范政务数据风险评估工作流程，明确政务数据风险评估各阶段的实施要点和工作方法，进一步提升保障能力，制定本评估指南

川渝政务数据风险评估指南

1. 范围

本文件规范提出了四川省、重庆市行政区域内开展政务数据风险评估的基本概念、要素关系、分析原理、实施流程、评估内容等。

本文件适用于指导四川省、重庆市各级政务部门开展政务数据风险自评估，同时适用于政务数据处理者、第三方开展政务数据风险评估，也可供主管监管部门实施政务数据风险评估时参考。

本文件适用于不涉及国家秘密的政务数据资源。

1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984—2022 信息安全技术信息安全风险评估方法

GB/T 21063.4-2007 政务信息资源目录体系 第4部分：政务信息资源分类

GB/T 25069—2022 信息安全技术术语

GB/T 37988—2020 信息安全技术数据安全能力成熟度模型

GB/T 39335—2020 信息安全技术个人信息安全影响评估指南

TC260-PG-20231A 网络安全标准实践指南—网络数据安全风险评估实施指引

DB51/T 3056-2023 政务数据 数据分类分级指南

DB51/T 3058-2023 政务数据 数据脱敏规范

1. 术语和定义

GB/T 25069、DB51/T 3056-2023 、DB51/T 3058-2023界定的以及下列术语和定义适用于本文件。

3.1政务数据 government affairs data

各级政务部门及其技术支撑单位在履行职责过程中依法采集、生成、存储、管理的各类电子数据资源。

3.2政务数据处理活动 government affairs data processing activities

政务数据收集、存储、使用、加工、传输、提供、公开、出境、删除等活动。

3.3政务数据处理者 government affairs data processor

政务数据处理者是指在政务数据处理活动中自主决定处理目的和处理方式的各级政务部门、软件和信息技术服务企业等政务领域各类主体。

3.4政务数据安全 government affairs data security

通过采取必要措施，确保政务数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.5政务数据安全风险 government affairs data security risk

由于开展政务数据处理活动不合理、缺少有效的数据安全措施等，导致数据安全事件的发生的可能性及其对国家安全、公共利益或者组织、个人合法权益造成的影响。

3.6政务数据风险评估government affairs data risk assessment

对政务数据和政务数据处理活动的安全风险和违法违规问题进行检测评估的过程。

3.7合理性rationality

是指政务数据处理活动遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，不危害国家安全、公共利益，不得损害个人、组织的合法权益。

3.8安全措施security measure

保护政务数据和政务数据处理活动、抵御数据安全风险事件而实施的各种安全管理和技术实践、规程和机制。

3.9业务business

组织为实现某项发展战略而开展的运营活动，该活动具有明确的目标，并延续一段时间。

3.10风险源risk source

可能导致危害政务数据和政务数据处理的保密性、完整性、可用性和合理性等安全事故的原因、条件、情形或行为。

注：风险源，既包括安全威胁利用脆弱性可能导致政务数据安全事件的风险源（简称为“政务数据安全风险源”），也包括政务数据处理活动不合理操作可能造成违法违规处理事件的风险源（简称为“违法违规处理风险源”）。

1. 政务数据风险评估工作概述
	1. 评估思路

政务数据风险评估坚持预防为主、主动发现、积极防范，要对政务数据处理者的数据和数据处理活动中可能影响政务数据保密性、完整性、可用性和政务数据处理活动合理性的安全风险进行分析和评价。政务数据安全风险评估的评估思路如图1 所示。

图1 政务数据安全风险评估思路示意图

政务数据安全风险评估，主要围绕政务数据和政务数据处理活动，聚焦可能影响政务数据的保密性、完整性、可用性和数据处理合理性的安全风险。首先通过信息调研识别政务数据处理者、业务和信息系统、政务数据资产、政务数据处理活动、安全防护措施以及网络安全等级保护测评、密码应用安全评估等国家法律法规、强制性国家标准等文件要求的检测评估工作情况等相关要素然后从政务数据安全管理、政务数据处理活动、政务数据安全技术、个人信息保护、检测评估结果等方面进行风险评估，从国家安全、公共利益、行业组织或个人合法权益等方面综合分析，最后梳理风险问题清单和风险评估报告，并给出整改建议。

政务数据风险评估涉及政务数据、政务数据处理活动、业务、安全措施、政务数据安全风险等基本要素，如图2所示，此图不涉及流程顺序，仅展示要素间关系。

图2 政务数据风险评估要素关系

开展政务数据安全风险评估应充分考虑要素间关系。各关键要素关系说明如下：

a) 政务数据是核心要素，具有数据价值等属性，数据价值将影响数据安全风险的危害程度。

b) 政务数据和政务数据处理活动是政务数据安全风险评估的评估对象。

c) 业务需要依托信息系统的支撑，可能涉及一个或多个信息系统。

d) 信息系统包含多个政务数据处理活动，信息系统是政务数据的载体。

e) 政务数据在流转过程中涉及一个或多个政务数据处理活动，政务数据处理活动应遵循数据安全法律法规要求。

f) 安全措施用于保护政务数据安全，能降低数据安全风险源发生的可能性。

g) 政务数据和政务数据处理活动作为评估对象，可能存在风险源，风险源可能引发数据安全风险，数据安全风险将对政务数据和政务数据处理活动有潜在影响。

* 1. 评估适用情形

核心数据的界定和保护要求按照国家相关文件执行。

符合以下情形之一的政务数据处理者，需结合实际情况开展政务数据风险评估：

a) 党政机关、事业单位、国有企业等涉及重要数据、关键信息基础设施运营、100 万人以上个人信息、大型互联网平台运营的政务数据处理者，宜每年至少开展一次政务数据风险评估；

b) 政务数据处理者在重要数据共享、交易、委托处理或向境外提供前，应开展政务数据风险评估；

c) 政务数据处理者开展高风险政务数据处理活动前，宜开展政务数据风险评估。

风险评估工作是持续性的活动，当评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生变化时，应重新开展风险评估。

* 1. 评估内容框架

政务数据风险评估内容，既包括涉及政务数据处理者、业务和信息系统的基本情况调研，也包括处理的政务数据、开展的政务数据处理活动情况识别，还包括政务数据处理活动、政务数据安全管理、政务数据安全技术、个人信息保护、重要数据处理等方面的评估内容，评估内容框架如图3所示。

图3 政务数据风险评估内容框架图

* 1. 评估实施流程

政务数据风险评估实施流程，主要包括评估准备、政务数据和政务数据处理活动识别、风险识别、风险分析与评价、评估总结五个阶段，如图4 所示。

图4 政务数据风险评估实施流程图

* 1. 评估工作形式

从实施主体来区分，政务数据风险评估分为自评估和检查评估，具体实施步骤可参考附录A。

自评估是指四川省、重庆市各级政务部门根据政务数据风险评估适用情形自行发起对政务数据资产和政务数据应用场景的评估，自评估可以指定内部专门负责评估、审计的岗位或角色开展，也可以委托外部专业机构开展评估工作。

检查评估是指四川省、重庆市各级政务部门的上级监管单位发起的政务数据风险评估工作，上级监管单位是指有直接领导关系或负有监督管理责任的部门，也可以委托第三方专业机构开展评估。

* 1. 评估手段

开展数据安全风险评估时，综合采取人员访谈、文档查验、安全核查和技术检测等手段进行评估。

1. 政务数据风险评估工作实施
	1. 评估准备
		1. 确定评估目标及范围

明确政务数据风险评估的目标，根据评估目标确定政务数据风险评估的对象、范围和边界，明确评估涉及的政务数据资产、政务数据处理活动、业务、信息系统、人员和内外部组织等。

政务数据风险评估对象主要是政务数据和政务数据处理活动，工作范围可能是全部政务数据及政务数据处理活动相关的各类资产和部门，也可能是某个独立的业务、信息系统、政务数据资产、政务数据处理活动或部门等。

1. 新建的等保测评三级及以上的政务系统、最低安全级别三级及以上的政务数据，应至少选取三个类别政务数据及其政务数据处理活动开展自评估；
2. 已建设完成或等保测评二级及以下的政务系统、最低安全级别二级及以下的政务数据，由系统和政务数据运行管理方按评估适用情形自行确定。
	* 1. 组建评估团队

根据评估目标和评估范围，组建政务数据风险评估团队，由评估管理单位、评估方、评估对象等相关人员组成，必要时也可邀请有经验的政务数据安全专家组成专家组。

a) 评估对象通常由组织的政务数据安全负责人和安全、法务、合规、运维、研发、业务等部门相关人员组成；

b) 如需选择第三方，应确保具备政务数据安全评估能力；

c) 评估方应做好评估前的表格、文档、检测工具等各项准备工作，并按照需求签署保密协议。

* + 1. 开展前期调研

对评估对象的数据资产、政务数据处理活动、检测评估、安全措施、业务、信息系统、人员和内外部组织政务数据处理者及被评估的业务和信息系统基本情况等进行调研。

* + 1. 制定评估实施方案

根据评估目标、评估范围和调研情况，明确政务数据风险评估的评估依据、评估内容和评价准则，形成政务数据风险评估方案。

* 1. 政务数据和政务数据处理活动识别
		1. 政务数据识别及分类分级

针对被评估的业务和信息系统，识别政务数据处理情况，输出政务数据情况清单，如表1所示。

**表1 政务数据情况清单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 政务数据名称 | 政务数据编号 | 政务信息资源分类 | 行政许可事项名称 | 来源信息系统 | 升降级措施 | 数据安全级别 |
|  |  |  |  |  |  |  |  |

* + 1. 政务数据处理活动识别

针对被评估的业务或政务数据，识别开展的政务数据处理活动情况，输出政务数据处理情况清单，如表2所示。

**表2 政务数据处理活动清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 政务数据名称 | 政务数据编号 | 政务数据处理活动类别 | 政务数据处理活动描述 |
|  |  |  |  |  |

* 1. 政务数据安全风险识别
		1. 概述

政务数据安全风险识别，主要围绕政务数据安全措施、政务数据安全风险源和违法违规处理风险源，通过对政务数据处理活动、政务数据安全管理、政务数据安全技术、个人信息保护、重要数据处理安全等方面进行评估，发现可能存在的政务数据安全问题和风险隐患。具体实施时可按照以下步骤开展：

a） 如果评估对象已开展过相关的测评工作，应先对已开展的测评工作结论进行分析；

b） 评估对象应从政务数据处理活动（见5.3.3）、政务数据安全管理（见5.3.4）、政务数据安全技术（见5.3.5）、个人信息保护（见5.3.6）、重要数据处理（见5.3.7）等方面，进行评估；

c） 梳理各评估项的评估结果和发现的风险问题，输出政务数据风险评估记录。

* + 1. 已开展测评工作结论分析

评估对象应当按照国家法律法规、强制性国家标准等文件要求，通过有关检测评估，包括但不限于网络基础环境、密码应用等。在开展风险评估时，应记录评估对象应开展的检测评估工作及实际开展情况，主要包括：

a) 政务数据处理活动涉及应开展检测评估工作名称、要求来源等基本情况；

b) 已开展检测评估工作有效性（指是否由有资质机构，按照正常程序开展）；

c) 在用软件产品安全测试报告、已有安全漏洞验证；

d) 检测评估内容和结果，及检测评估工作开展情况。

已开展检测评估工作情况应由评估对象提供证明材料，评估人员通过访谈、检查、测试等方式验证证明材料真实性、有效性，并对检测评估已发现且暂未整改或未采取有效措施进行缓解的问题，进行梳理归类，根据问题属性，作为不同类别风险源识别依据。

若评估对象未实施或通过国家法律法规、强制性国家标准等文件要求的检测评估工作，如网络安全等级保护测评、密码应用安全性评估、云计算服务安全评估、互联网信息服务算法推荐安全评估、数据出境安全评估等，则判定存在未按要求开展检测评估工作的安全风险。

* + 1. 政务数据处理活动风险源识别

政务数据处理活动风险源识别，主要针对政务数据生命周期各处理环节中的操作，发现可能存在的政务数据收集安全风险和违法违规问题，掌握政务数据安全防护措施部署情况，常见风险源如表3所示。

**表3 政务数据处理活动风险源表**

|  |  |
| --- | --- |
| 风险源类别 | 风险源描述 |
| 政务数据收集 | 政务数据收集合法正当性、间接采集政务数据安全、自动采集政务数据安全、政务数据质量管理等。 |
| 政务数据存储 | 逻辑存储安全、存储介质安全、政务数据备份恢复等。 |
| 政务数据传输 | 政务数据传输加密、传输完整性保护、网络可用性等。 |
| 政务数据使用和加工 | 政务数据使用合法性、政务数据正当使用、政务数据导入导出安全、政务数据处理环境安全、政务数据加工安全等。 |
| 政务数据提供 | 政务数据提供合法性正当性必要性、政务数据提供安全管理、政务数据提供安全技术、政务数据接收方安全等。 |
| 政务数据公开 | 政务数据公开安全管理、敏感信息公开等。 |
| 政务数据删除 | 政务数据销毁安全、政务数据匿名化处理、存储介质销毁等。 |

* + 1. 政务数据安全管理风险源识别

政务数据安全管理风险源识别，主要从安全组织管理、制度流程、分类分级、人员安全、合作方管理、应急管理以及投诉举报等方面，发现可能存在的政务数据安全管理组织风险和违法违规问题，掌握政务数据安全组织管理情况，如表4所示。

**表4 政务数据安全管理风险源表**

|  |  |
| --- | --- |
| 风险源类别 | 风险源描述 |
| 政务数据安全组织管理 | 政务数据安全组织架构、政务数据安全岗位设置等。 |
| 政务数据安全制度流程 | 政务数据安全制度体系、政务数据安全制度管理等。 |
| 政务数据分类分级管理 | 政务数据资产管理、政务数据分类分级制度、政务数据分类分级保护等。 |
| 人员安全管理 | 人员录用、保密协议、转岗离岗、政务数据安全培训等。 |
| 政务数据合作方管理 | 合作方管理机制、合同协议约束、外包访问权限、第三方接入等。 |
| 政务数据安全应急管理 | 政务数据安全应急预案、应急处置、应急告知等。 |
| 政务数据安全投诉举报 | 政务数据安全投诉举报渠道、公布、处理等情况等。 |

* + 1. 政务数据安全措施风险源识别

政务数据安全技术风险源识别，主要从身份鉴别、访问控制、权限管理、政务数据安全风险监测、政务数据安全审计、政务数据脱敏、政务数据防泄漏等方面进行评估，对政务数据安全措施的有效性和完备性进行验证，发现可能存在的政务数据安全技术风险和违法违规问题。

* + 1. 个人信息保护风险源识别

根据《个人信息保护法》《App 违法违规收集使用个人信息认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法规政策要求，从个人信息处理合法正当、个人信息处理必要性、个人信息保护政策、告知同意、个人信息主体权利、App 个人信息保护等方面进行评估，发现可能存在的个人信息保护风险和违法违规问题。

* + 1. 重要数据保护风险源识别

根据《网络安全法》《数据安全法》《网络政务数据安全管理条例（征求意见稿）》等法律法规，从重要数据安全负责人和管理机构、政务数据风险评估、政务数据安全应急、政务数据安全培训、政务数据提供安全等方面进行评估，发现可能存在的重要数据处理安全风险或违法违规问题。

* 1. 政务数据安全风险分析与评价
		1. 风险分析

政务数据安全风险分析，主要在风险源识别和政务数据安全措施识别的基础上，分析各项风险源或问题可能带来的政务数据安全风险，风险一般可按照附录B所列21类风险进行归类,表5给出了风险分析示例。

**表5 政务数据安全风险分析（示例）**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 风险类型（面临的数据安全风险） | 保护要求（应对措施） | 可能导致的风险（应对措施有效程度） |
| 1 | 1）窃取或者以其他非法方式获取政务数据2）政务数据完成采集后，未按照合同要求使用政务数据，且将政务数据用于“大数据杀熟”，违反法律、行政法规规定的目的和范围内使用政务数据 | 1）具备合同、隐私政策等合法政务数据收集证据。（应对措施：以合同形式约定从外部机构采集的政务数据范围、收集方式、安全措施。）2）明确政务数据的采集渠道，规范政务数据采集格式、流程及方法。（应对措施：未明确政务数据的采集渠道，规范政务数据采集格式、流程及方法，未能采取措施保持政务数据源正式有效及采集过程的安全可控。） | 违法违规利用政务数据 |

* + 1. 风险评价
			1. 风险危害程度评价

风险危害程度评价，主要从政务数据安全风险一旦发生，对国家安全、公共利益或者个人、组织合法权益造成的危害程度进行评价，将风险危害程度从低到高分为很低、低、中、高、很高5个级别，如表6所示。

**表6 政务数据安全风险危害程度等级参考**

|  |  |  |
| --- | --- | --- |
| 等级 | 政务数据安全风险危害程度描述 | 对应政务数据分级等级 |
| 很高 | 一旦发生政务数据安全风险，对国民经济命脉、重要民生和重大公共利益造成损害。例如核心数据处理安全风险、关系3个以上重点行业领域的重要数据处理安全风险、存在严重的重要数据违法违规处理行为等。 | 四级 |
| 高 | 一旦发生政务数据安全风险，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。例如重要数据处理安全风险、超过100万人的个人信息处理安全风险、超过10万敏感个人信息违法违规收集使用行为等。 | 三级 |
| 中 | 一旦政务数据被泄露或篡改、损毁或者非法获取、非法利用，容易导致组织或个人的合法权益造成严重危害。例如敏感个人信息处理安全风险、组织知识产权和商业秘密处理安全风险、存在超过10万个人信息违法违规收集使用行为等。 | 二级 |
| 低 | 一旦发生政务数据安全风险，可能对组织或个人的合法权益造成中等危害。例如个人信息等。 | 一级 |
| 很低 | 一旦政务数据安全风险发生，可能导致组织或个人的合法权益造成轻微危害。通常为一般政务数据（非个人信息）、非敏感的组织政务数据等。 | 一级 |

* + - 1. 风险发生可能性评价

风险发生可能性评价，主要考虑风险隐患发生的可能性、安全措施有效性和完备性等因素，将政务数据安全风险发生的可能性从低到高分为低、中、高3 个级别，如表7所示。

**表7 风险发生可能性等级参考**

|  |  |
| --- | --- |
| 等级 | 风险发生可能性描述 |
| 高 | 涉及违法违规行为、缺少政务数据安全措施或安全措施有效性较弱，风险隐患发生可能性高（例如出现频率高、在大多数情况下几乎不可避免、可以证实经常发生过）。 |
| 中 | 有一定政务数据安全措施，但有效性不足，风险隐患发生可能性一般（例如出现频率中等，在某种情况下可能发生，或被证实曾经发生过）。 |
| 低 | 政务数据安全措施比较到位、完备，风险隐患发生可能性低（例如几乎不可能发生，或仅可能在非常罕见和例外的情况下发生）。 |

* + 1. 安全风险等级判定

综合风险危害程度及风险发生可能性的评价结果，结合评估对象实际情况，获得政务数据安全风险等级评定结果，表8给出了利用矩阵关系获取评定结果示例，评定结果包括：

a) 重大安全风险：一般指可能直接影响政治安全的政务数据安全风险；

b) 高安全风险：一般指可能直接危害国家安全、经济运行、社会稳定、公共健康和安全；

c) 中安全风险：一般指对自然人的人格尊严受到严重侵害或者人身、财产安全受到严重危害，对社会、公共权益有直接影响；

d) 低安全风险：一般指对自然人的人格尊严受到侵害或者人身、财产安全受到危害，对社会、公共权益有一定或较小影响；

e) 很低安全风险：一般指影响小范围的组织或公民个体权益，对人格尊严、人身安全、财产安全不造成侵害或仅产生较轻微的危害。

**表8 政务数据安全风险评价矩阵（示例）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 危害程度可能性 | 很高 | 高 | 中 | 低 | 很低 |
| 高 | 重大风险 | 高风险 | 高风险 | 中风险 | 低风险 |
| 中 | 重大风险 | 高风险 | 中风险 | 低风险 | 轻微风险 |
| 低 | 高风险 | 中风险 | 低风险 | 轻微风险 | 轻微风险 |

* + 1. 安全风险清单

针对各项政务数据安全风险完成风险评价后，整理各项风险评估结果，在5.4.1.1 的初步风险清单基础上形成政务数据安全风险清单（如表9所示），列出各项风险的风险等级、危害程度、发生可能性等，其中风险等级可按特殊情况或最新文件要求进行调整。

**表9 政务数据安全风险清单**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 风险类别 | 风险源或问题 | 风险描述 | 采取的安全措施 | 风险等级 | 风险危害程度 | 风险发生的可能性 | 涉及的政务数据 | 涉及的政务数据处理活动 | 评估情况描述 |
|  |  |  |  |  |  |  |  |  |  |  |

* 1. 评估总结
		1. 编制评估报告及评估得分

对评估结果进行分析总结，编制政务数据风险评估报告，报告模板参见附录B。无重大风险、高风险或重大风险、高风险全部处置完成后，可选择对评估结果进行量化评分，政务数据安全工作评估得分表模板参见附录C。

* + 1. 安全风险处置及开放共享建议

评估人员结合实际情况，对发现的政务数据安全风险提出处置建议，酌情指导政务数据处理者整改，跟踪风险处置情况，并开展风险复评估。政务数据处理者按照组织的风险接受规则，制定相应的政务数据安全风险处置方案。评估人员根据政务数据处理者决定的风险处置措施，结合风险识别和评估方法，预判措施有效性和残余风险，形成记录。根据评估结果，按数据共享、开放与安全级别的对应关系，给出政务数据共享开放建议。

附录A
（资料性）
自评估和检查评估实施步骤

图5 数据风险自评估实施步骤图



图6 数据风险检查评估实施步骤图

附录B
（资料性）
典型政务数据安全风险类别

**表B.1 典型政务数据安全风险示例表**

|  |  |
| --- | --- |
| 风险类别 | 描述 |
| 政务数据泄露风险 | 由于政务数据窃取、爬取、脱库、撞库等安全威胁，或者缺乏有效的安全措施、人员操作失误作或有意盗取等，导致政务数据被未授权泄露、访问从而影响政务数据保密性的风险； |
| 政务数据篡改风险 | 由于政务数据注入、中间人攻击等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致政务数据被未授权篡改等从而影响政务数据完整性的风险； |
| 政务数据破坏风险 | 由于拒绝服务攻击、自然灾害、嵌入恶意代码、政务数据污染、设备故障等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致政务数据被破坏、毁损、政务数据质量下降等从而影响政务数据可用性、准确性的风险； |
| 政务数据丢失风险 | 由于政务数据过载、软硬件故障、备份失效、链路过载等问题，或者缺乏有效的安全措施、人员有意或无意操作等，导致政务数据被丢失、难以恢复等从而影响政务数据可用性的风险； |
| 政务数据滥用风险 | 由于缺乏授权访问控制、权限管控等有效的安全管控措施、人员有意或无意操作等，导致政务数据被未授权或超出授权范围使用、加工的风险； |
| 政务数据伪造风险 | 由于政务数据源欺骗、深度伪造等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致政务数据或政务数据源被伪造、政务数据主体被仿冒等安全风险； |
| 违法违规获取政务数据 | 违反法律、行政法规等有关规定，非法或违规获取、收集政务数据的风险； |
| 违法违规出售政务数据 | 违反法律、行政法规等有关规定，非法或违规向他人出售、交易政务数据的风险； |
| 违法违规保存政务数据 | 违反法律、行政法规等有关规定，非法或违规留存政务数据的风险，如逾期留存、违规境外存储等； |
| 违法违规利用政务数据 | 违反法律、行政法规等有关规定，非法或违规使用、加工、委托处理政务数据的风险； |
| 违法违规提供政务数据 | 违反法律、行政法规等有关规定，非法或违规向他人提供、共享、交换、转移政务数据的风险； |
| 违法违规公开政务数据 | 违反法律、行政法规等有关规定，非法或违规公开政务数据的风险； |
| 违法违规购买政务数据 | 违反法律、行政法规等有关规定，非法或违规购买、收受政务数据的风险； |
| 违法违规出境政务数据 | 违反法律、行政法规等有关规定，非法或违规向境外提供政务数据的风险； |
| 超范围处理政务数据 | 政务数据处理活动违反必要性原则，超范围或过度收集使用个人信息或重要数据的风险； |
| 政务数据处理缺乏正当性 | 违反正当性原则，政务数据处理活动缺乏明确、合理的处理目的； |
| 未有效保障个人信息权益 | 由于未采取有效的个人信息保护措施、人员操作或外部威胁等，导致未能有效保障个人信息主体的知情权、决定权、限制或者拒绝个人信息处理等个人信息合法权利； |
| 政务数据处理缺乏公平公正 | 由于缺乏安全管控措施、人员有意或无意操作等，导致政务数据处理违反公平公正、诚实守信原则，侵犯其他组织或个人合法权益的风险； |
| 政务数据处理抵赖 | 由于外部攻击威胁、缺乏有效安全管控措施、人员有意或无意操作等，导致处理者或第三方否认政务数据处理行为或绕过政务数据安全措施等风险； |
| 政务数据不可控 | 由于第三方政务数据安全能力不足、缺乏有效的第三方管控措施、合同协议缺失、外包人员操作等，导致委托处理或合作的第三方违反法律法规或合同协议约定处理政务数据，造成第三方超范围处理政务数据、逾期留存政务数据、违规再转移等政务数据不可控风险； |
| 其他风险 | 其他可能影响国家安全、公共利益或组织、个人合法权益的政务数据安全风险。 |

附 录 C
（资料性）
政务数据风险评估报告模板

一、评估概述

1.1 评估目的和依据

1.2 评估对象和范围

1.3 评估结论概要

（政务数据和政务数据处理活动的概要情况，评估结果及处置建议概要。）

二、评估工作开展情况

2.1 评估工作组织情况

（概要说明为开展本次评估工作，单位内部建立的组织机构及其人员构成、相关工作机制、汇报机制等工作组织情况。）

2.2 评估时间安排情况

（对本次评估工作的时间进度安排进行说明，对每个工作阶段的工作内容、消耗时间、工作结果等信息进行描述。）

2.3 参与人员情况

（对本次评估工作的参与人员和部门进行说明）

三、政务数据和政务数据处理活动识别

3.1 政务数据处理者基本信息

3.2 业务和信息系统情况

3.3 政务数据情况（至少包含种类、数量等信息）

3.4 政务数据处理活动开展情况

3.5 政务数据安全历史事件情况

四、政务数据安全风险识别

4.1 已开展安全测评结果分析

4.2 政务数据处理活动安全风险识别

4.3 政务数据安全管理风险识别

4.4 政务数据安全技术风险识别

4.5 个人信息保护风险识别（如有）

4.6 重要数据处理安全风险识别（如有）

五、风险分析和评价

5.1 政务数据安全风险整体情况

5.2 政务数据安全风险分析（至少包含面临的数据安全风险及其应对措施的有效程度等）

5.2 政务数据安全风险清单

六、风险处置建议和残余风险分析

7.1 风险处置建议

7.2 残余风险分析及政务数据开放共享建议

附件 1 政务数据情况清单

附件 2 政务数据处理活动清单

附 录 D
（资料性）
政务数据安全工作评估得分表模板

**表D.1 政务数据安全工作评分得分表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评估内容 | 评估情况 | 评估得分（满分100分，对照政务数据安全风险清单进行扣分，数据安全风险等级每有一项中风险扣2分、低风险扣1分、轻微风险扣0.5分） |
| 1 | 已开展测评工作结论分析 |  | 满分15分 |
| 2 | 政务数据处理活动风险 |  | 满分30分 |
| 3 | 政务数据安全管理风险 |  | 满分20分 |
| 4 | 政务数据安全措施风险 |  | 满分10分 |
| 5 | 个人信息处理风险 |  | 满分10分 |
| 6 | 重要数据处理风险 |  | 满分15分 |

备注：无重大风险、高风险或重大风险、高风险全部处置完成后，可选择对评估结果进行量化评分。

参 考 文 献

参考文献

[1]中华人民共和国网络安全法（2016年11月7日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过）

[2]中华人民共和国数据安全法（2021年6月10日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过）

[3]中华人民共和国个人信息保护法（2021年8月20日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过）

[4]关键信息基础设施安全保护条例（2021年4月27日国务院第133次常务会议通过）

[5]四川省数据条例（2022年12月2日四川省第十三届人大常委会第三十八次会议审议通过）

[6]重庆市数据条例（2022年3月30日重庆市第五届人大常委会第三十三次会议审议通过）

[7]四川省省级政务信息化项目管理办法（2021年10月5日发布）

[8]重庆市政务数字化应用管理暂行办法（2023年7月14日印发）

[9]GB/T 20984-2022 信息安全技术 信息安全风险评估方法

[10]GB/T 35273—2020 信息安全技术 个人信息安全规范

[11]GB/T 37988—2019 信息安全技术 政务数据安全能力成熟度模型

[12]GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

[13]YD/T 3801-2020 电信网和互联网政务数据风险评估实施方法

[14]JR/T 0223-2021 金融政务数据安全 政务数据生命周期安全规范